Network security

Technology, Computer

Network security and management is becoming increasingly important as file sharing becomes more popular amongst computer users. As advances are made in networkingtechnologyallowing for innovations such as wireless network access, a huge security issue has been raised with past solutions being inadequate to deal with today's issues. This research paper will examine and compare journal papers currently looking at this issue and attempt to give an increased insight into the problem. Introduction The idea of networking started out as a way to share files and resources.

With simple connection such as peer-to-peer access via a serial cable, and later on network cards, security was not really an issue. People only shared files and resources so tacks only came from internal sources such as transportable media like 3. 5" floppy disks. They could transport viruses whether purposely brought or not. Thus if you needed to secure your network you would buy an anti-virus package. With the introduction of the Internet came an entirely new threat. The Internet opened up the possibilities of malicious attacks from remote computers. An anti-virus package was not enough so further tools such as firewalls were required.

The Internet allows us to do more and more each day with the advent of innovations such as Internet shopping and e-mail, we have opened our computers and private information to many security threats. Recent technological strides such as wireless networking further aggravate this problem by making the security threat itself mobile. So how can we safeguard ourselves against these attacks? To answer this question I have compared two journal papers. The references to these papers can be found

in the bibliography. Findings The papers I have researched have highlighted the following points with regards to network security.

Firewalls Firewalls are an essential part of securing a network. They exist in various forms and deal with security in a variety of ways. Firewalls basically work by monitoring ports on your computing for any outside locations trying to access your computer. Firewalls come in hardware and software versions. Both have their good and bad points but generally hardware firewalls offer better security, as they are devoted to doing that job. Ellison makes a good point about securing your firewall saying, "... passwords with which it was shipped need to be changed to very secure, hard to guess, passwords.

These passwords can be written down, because they are defending against network hackers... " (Home Network Security Journal, C. M. Ellison, page 2) The point he is making is that your firewall needs to be secure as well. The password you use as the firewall administrator should be an extremely long and complex password so it is impossible to guess. The password can be stored on paper in your home because the firewall is protecting against outside attacks. Firewalls do not solve all problems though. They can cause programs not to work if the program uses a certain port.

The problem is getting a balance between security and freedom. The more secure the system is the less freedom you have. The main problem though, is that with the introduction of wireless every device will need its own firewall. If you have a network system running from a server then the server is likely to have a firewall to prevent anything outside of the network accessing it. What about internal attacks? A wireless device can access any

device that can receive wireless signals. This means that each internal device needs its own firewall or form of security. Wireless connections

Wireless security uses cryptographic keys to identify devices. Wireless devices are becoming popular as they allow you the freedom to roam whilst still being connected to a network. Many points raised with regards to Wireless security are associated with the authentication of devices on a network. Most of the problems occurring in current wireless technology are due to the weaknesses in WEP (Wired Equivalent Privacy). Regan identifies that "... known weaknesses in WEP mean that the keys should be changed frequently... " WEP is the algorithm used in IEEE 802. 11b (the most common wireless network standard) to encrypt traffic.

Thus this algorithm needs to be secure however, Regan points out that "... because WEP has inherent weaknesses it is not sufficient to rely on static WEP keys... they may need to be changed as frequently as every 10 minutes". Regan comments on how impractical this is to large businesses. In the WEP algorithm a key is made available to the client and the AP (authorisation protocol). Only if these keys match can the client be granted access to the network. We can see that the weaknesses in WEP that allow the key to be obtained could cause very real problems for companies using the WEP algorithm.

Regan points out the WEP security problem thus "... it is possible to derive the secret WEP key from the key steam... " (K, Regan, 'Wireless LAN Security: Things You Should Know about WLAN Security', page 3) Authentication This is perhaps the most important aspect of network

security. Without it there would be no way of identifying devices on a network securely. Authentication of devices is used in firewalls, sending and receiving e-mails, accessing secure locations etc. One form of Authentication relies on the distribution of keys.

The need for keys arises from the lack of safety in simple security measures such as passwords. Passwords have always been a problem in security. People generally choose a password of significance to themselves. The problem with this is that if information is gathered about that person then a password can normally be deduced. As Ellison states " If they can be memorized, they are probably to simple and so can be guessed; if they are to complex, they are written down and are therefore available to a passer by" (Ellison, Home Network Security Journal, page 7). Keys mechanisms work in a variety of ways.

The problem with any form of identification involving a key or password is it often static and so it gives a hacker the chance to guess it. It is important with any password/key system to regularly change it. Analysis Both papers focus on network security issues with the paper 'Home Network Security' by C, M, Ellison taking an overall view of networking and concentrating mainly on Authorisation and Authentication. The second paper 'Wireless LAN Security: Things You Should Know about WLAN Security' by K, Regan focuses on Wireless Networking, which is the area that has created a lot of security issues recently.

Like the paper by Ellison it concentrates on Authentication. Initial analysis of the papers would suggest they are quite different from one another in their

primary focus but in fact what they both highlight, in slightly different ways, is the need for secure and adequate authentication of devices on a network both internally and remotely. As K, Regan quite rightly points out in his Summary " A good authentication framework is vital, and will form the heart of a secure WLAN". Other points K, Regan raises are the three types of Authentication used in Access Points.

The first Regan highlights as " Open authentication" which is as it sounds allowing any client to access the network. Regan points out that this should only generally be used in public places where any one may need to access the system and is such a case "... a second authentication system is then used". This second system could be anything from a password to an IP check. The second type of Authentication used is " Shared authentication". This shares WEP (Wired Equivalent Privacy) keys with the clients and the AP (Access Point, as stated above). When the client and AP keys match access is granted.

Regan goes on to explain that there are known weaknesses in the system and one floor in particular allows an intruder to obtain the key. This means that Keys have to be changed regularly. The final type of AP authentication used is " Network-EAP". This uses one of the EAP (Extensible Authorisation Protocol) methods such as LEAP used by Cisco. The Authentication issues discussed in C, M, Ellison's paper centre around digital signatures and MAC (Message Authentication Code). Digital signatures are where "... only the sender needs a copy of that secret key in order to get maximum security".

The sender encodes the message and then the receiver checks that only someone in possession of the correct key could have produced the message. MAC Authentication is where the both sender and receiver have a copy of the key. This is faster than digital signatures but as Ellison points out " Because there are two or more copies of that value... there is more opportunity for it to be compromised... " It is Ellison who points out the differences between Authentication and Authorisation. He rightly tells us " Until you have established both authentication and authorisation, you cannot make a security decision...

" By this he means that once we have concluded that the message came from a legitimate source, we need to check that the source in question is allowed to access the service it is trying to access. This is a minor point but one that is important to networks as it allows a tired level of security governed by access rights and privileges, Ellison goes into further detail by explaining some available authorisation methods to determine who has access to what. K, Regan, doesn't make the importance of authorisation clear in his paper.

This is partly because the paper is aimed at professionals and so it is assumed the reader will know. The authorisation methods described by Ellison are ACL (Access Control List), Authorisation server, and authorisation certificate. The ACL resides in memory in the device where the accessed resource is stored. It is a series of entries containing information about the subject (the entity being granted access), authorisation (the rights being

granted), delegation (indicates whether subject can delegate the rights), and validity (this can include a time of access expiration).

The second authorisation method is the authorisation server. This method of authorisation is where the ACL is stored on a serve. It is particularly valuable in corporations with many machines. Access requests are sent to the authorisation server, which then sends its reply. However, each client machine needs a single ACL entry to validate the authorisation server. The final authorisation method is the authorisation certificate. This is a digitally signed ACL entry. This method is somewhat more complex and involves the use of delegation. Evaluation

Initial evaluation shows the shows the 'Home Network Security' journal by Ellison to be the most concise offering by delving into many aspects of security. The point the author is making is that the security of a home network can be more complex than that of a corporate network. The home user is attempting to secure a system that in a corporation is secured by physical guards. This is a valid point but seems somewhat unimportant. The real question is whether a user has the will to implement this security system. Ellison also concludes that "... network security thinking to date has assumed that network access is binary...

Where you either allow access to the system or you don't. In fact " The idea of controlling access to individual components is relatively new... " The point being made here is that network security is not a simple case of allowing or disallowing access, but instead, it deals with shades of security whereby the system must control which resources a client can access individually.

Ellison's journal paper is concise and provides a good foundation for home network users. It gives a clear insight into current methods and suggests areas of weakness.

Moving on to the second Journal paper 'Wireless LAN Security: Things You Should Know about WLAN Security' by K, Regan. We see a more focused approach. This paper deals with wireless network security. In essence this is a follow up to Ellison's paper, offering answers to the problem of future network security. I believethat many points raise in Regan's paper also apply to wired security and as devices appear that cater for both technologies (i. e. Ethernet wireless routers), so the answers to security problems will merge into a single solution. Regan gives a clear insight into current wireless security measures.

He clearly explains how wireless security is dealt with currently and points out the area he believes to be the future solution to these problems by concluding " A good authentication framework is vital... with dynamic key rotation and the forthcoming WPA/IEEE 802. 11i enhancements... weaknesses can be overcome". Regan suggests, as did Ellison, that the answer to arising and future network security issues is the advancement of authentication and authorisation issues creating ways to always be able to identify a client whilst keeping the key that does this in a non-fixed state.

Overall I believe that K, Regan's paper provides a much more useful and future focussed insight into network security issues and highlights the importance of authentication in wireless network systems. Conclusion In conclusion, it seems that authentication of devices is important in securing a

network. Without this other software and devices cannot block incoming attacks easily. Advancements made in authentication will allow updates in the effectiveness of firewalls and other security software.

Home users and small businesses are often unwilling to put time andmoneyinto security devices because they feel that the costs are too high for the information they need to secure. Unless smaller companies and individuals are willing to implement security measures then hackers and other malicious sources will always find ways to attack systems and spread dangerous code. It may be that manufacturers need to force security upon the end user by including it in devices as standard so that security exists regardless of whether the user takes an active role in its existence.

Recommendations The first journal gives a really good insight into basic security measures currently being used in network security. However, the second journal surpasses it by dealing with an extremely prominent subject (and the cause of many current security flaws). I feel K, Regan's paper will provide the best insight into how to deal with the wireless security threats and as wireless becomes more common, so the paper will be an even more valuable source of information with its points about authorisation really showing themselves to be true.